PROCEDURE 1350.20

Issued Date: April 30, 2006
Effective Date: May 31, 2006

SUBJECT: **Authorization prerequisite for access to protected data resources.**

APPLICATION: This procedure applies to all Executive Branch Departments, Agencies, Boards or Commissions using State information technology resources including, but not limited to, networks, systems, computers, databases, and applications.

This procedure does not apply to general public access to public or open information presented in HTML, voice, video, TTD, or other web compatible formats over the Internet or through the public switched telephone network.

PURPOSE: To establish, document, and manage the allocation of user access rights for individuals accessing State of Michigan information technology resources to prevent inadvertent and inappropriate access to resources not authorized for the individual user.

CONTACT AGENCY: Department of Information Technology (DIT)
Office of Enterprise Security

TELEPHONE: 517/241-4090

FAX: 517/241-2013

SUMMARY: This procedure requires the creation, documentation and management of unique user identification, and related password, for access to State information technology resources over the entire user access life cycle.

APPLICABLE FORMS: *[Request form for User ID, Password and Access to Authorized Identified IT Resources]*

PROCEDURES:

A. All users approved to access State information technology are subject to verification of identity credentials.

B. Each user, including external contracted service providers, will be assigned a unique end-user-ID or user-name, related password, and access rights using the following procedure:

1. The form to request the creation of a user ID, password, and access to identified State information technology resources is completed and signed by the end user seeking access.
2. The Agency information owner for the identified information technology resource(s) approves the request form for each individual user.

3. The form is transmitted to DIT for creation of the user ID, password, and implementation of the technical requirements for access to the identified information technology resources.

C. User responsibilities:

1. The user is responsible for all activity performed with their personal user ID.
2. User IDs and related password controls shall not be shared or used by anyone but the individual to whom issued.
3. Users are prohibited from allowing others to perform any activity with IDs belonging to other users.
4. Users shall not perform any activity with IDs belonging to other users.
5. Users shall sign an agreement acknowledging their understanding of the provisions of the State of Michigan Acceptable Use Policy and committing to maintain the confidentiality of the data to which they are authorized access.

D. Agency responsibilities:

1. Maintain documentation of authorized users from the initial request for creation of user ID and access to the final de-registration of users who no longer require access to State of Michigan protected information technology resources.
2. Periodically reevaluate the access privileges granted to users, to include whether currently enabled access privileges are still necessary to perform the user's current job duties.
3. Promptly report all significant changes in end-user duties or employment status to DIT and request change as necessary.
4. Request DIT terminate all State information systems privileges within 48 hours of the time that an employee, contract worker, agent, or volunteer ceases to provide services to the State of Michigan or when a change in agency or assigned work status occurs.
5. Request DIT de-commission a user-ID within forty-eight hours of termination of employment or services with the State of Michigan.
6. Limit in scope of access and by time of day and length of authorized access interval any anonymous user-IDs (such as "guest").
7. Identify, document, and coordinate with DIT appropriate user access levels associated with identified IT resources. Additionally:
    a. Coordinate with DIT-OES to accredit systems, applications, and resources to ensure business process controls and authorization requirements are met,
    b. Authorize and document group membership styles of access levels to facilitate access management, provided the groups are made up of identified (named) members.
    c. Authorize and document access by identified job profiles to minimize administration in appropriate cases where physical controls or supervisory processes can eliminate the likelihood of un-authorized access.

d. Certify and periodically audit membership for a given IT resource or application.
e. Supervise and control computer terminals with direct access though a combination of physical security measures and access rosters.

E. DIT responsibilities:

1. Manage the authorization procedures using the following life cycle steps.
    a. Identity verification
    b. Enrollment
    c. Routine use
    d. Transaction management
    e. Records management
    f. Testing
    g. Suspension, revocation, & re-issuance
    h. Audit
    i. De-registration, or termination
2. Not grant system application privileges to any user without specific written approval from the Agency information owner.
3. Issue user ID and related password.
4. Implement the technical requirements for granting access rights or privileges.
5. Terminate, change or de-commission user ID, password and/or access within 48 hours of receipt of request by Agency.
6. Certify fully functioning implementation of access as authorized.
7. Certify compliance with established IT security policies, standards and procedures.
8. Through DIT Office of Enterprise Security, review and monitor procedure to ensure appropriate authorization methods are implemented and take actions necessary to ensure compliance with State of Michigan IT security policies, standards, and procedures.
9. Through Internal Auditor, conduct periodic audits of IT resources for appropriate controls to maintain compliance with policy and standards.

F. State agencies desiring to implement practices and procedures differing from this procedure may do so only with the written approval of the DIT Office of Enterprise Security.

.

Authority is The Management and Budget Act, Public Act 431 of 1984, as amended, § 203.

* * *